International Journal of Number Theory
Vol. 15, No. 9 (2019) 1793–1800

DOI: 10.1142/S1793042119501008

A conjecture of Gross and Zagier: Case $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/3\mathbb{Z}$

Dongho Byeon
Department of Mathematical Sciences
Seoul National University Seoul, Korea
dhbyeon@snu.ac.kr

Taekyung Kim
Center for Geometry and Physics
Institute of Basic Science Pohang, Korea
Taekyung.Kim.Maths@gmail.com

Donggeon Yhee
Department of Mathematical Sciences
Seoul National University Seoul, Korea
dgyhee@gmail.com

Received 7 February 2019
Accepted 8 April 2019
Published 11 June 2019

Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N, c the Manin constant of E, and m the product of Tamagawa numbers of E at prime divisors of N. Let K be an imaginary quadratic field where all prime divisors of N split in K, P_K the Heegner point in $E(K)$, and III(E/K) the Shafarevich–Tate group of E over K. Let $2u_K$ be the number of roots of unity contained in K. Gross and Zagier conjectured that if P_K has infinite order in $E(K)$, then the integer $c \cdot m \cdot u_K \cdot |\mathrm{III(E/K)}|^{\frac{1}{2}}$ is divisible by $|E(\mathbb{Q})_{\mathrm{tor}}|$. In this paper, we show that this conjecture is true if $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/3\mathbb{Z}$.

Keywords: Elliptic curves; Manin constant; Tamagawa number; Shafarevich–Tate group.

Mathematics Subject Classification 2010: 11G05

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N, $X_0(N)$ the modular curve of level N and $\phi : X_0(N) \to E$ a modular parametrization. Let c be the Manin constant of E and $m = \prod_{p|N} m_p$, where m_p is the Tamagawa number of E at a prime divisor p of N.

Let K be an imaginary quadratic field with fundamental discriminant D_K, where all prime divisors of N split in K and $\mathcal{O}_K$ be the ring of integers in K. Then there exists a Heegner point x of discriminant D_K of $X_0(N)$, which corresponds to a pair of two N-isogenous elliptic curves with the same ring $\mathcal{O}_K$ of complex multiplication. The point x is defined over the Hilbert class field H of K. Put $P_K = \sum_{\sigma \in \mathrm{Gal(H/K)}} \phi(x)^\sigma$. Then $P_K \in E(K)$.

Let $L(\mathrm{E/K}, s)$ be the L-series of E over K and $\text{Ш}(\mathrm{E/K})$ be the Shafarevich–Tate group of E over K. Gross and Zagier [6] obtained a formula for the value of $L'(\mathrm{E/K}, 1)$ in terms of the height of P_K. Kolyvagin [10] proved that if P_K has infinite order, then $E(K)$ has rank 1 and $\text{Ш}(\mathrm{E/K})$ is finite.

Let $2u_K$ be the number of roots of unity contained in K. We note that $u_K = 1$ for all imaginary quadratic fields K except when $K = \mathbb{Q}(\sqrt{-1})$ and $K = \mathbb{Q}(\sqrt{-3})$, where $u_K = 2$ and $u_K = 3$, respectively.

The formula of Gross and Zagier, when combined with the conjecture of Birch and Swinnerton–Dyer, gives the following conjecture.

Conjecture 1 ([6, (2.2) Conjecture, p. 311]). *If P_K has infinite order in $E(K)$, then*

$$[E(K) : \mathbb{Z}P_K] = c \cdot m \cdot u_K \cdot |\text{Ш}(\mathrm{E/K})|^{\frac{1}{2}}.$$

Since $[E(K) : \mathbb{Z}P_K]$ is divisible by $|E(\mathbb{Q})_{\mathrm{tor}}|$, Gross and Zagier [6] suggested the following weaker conjecture.

Conjecture 2 ([6, (2.3) Conjecture, p. 311]). *If P_K has infinite order in $E(K)$, then the integer $c \cdot m \cdot u_K \cdot |\text{Ш}(\mathrm{E/K})|^{\frac{1}{2}}$ is divisible by $|E(\mathbb{Q})_{\mathrm{tor}}|$.*

Rational torsion subgroups of elliptic curves E over $\mathbb{Q}$ are completely classified by Mazur [13]: $E(\mathbb{Q})_{\mathrm{tor}}$ is isomorphic to one of the following 15 groups:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{for } 1 \le n \le 10, \ \ n = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} & \text{for } n = 2, 4, 6, 8. \end{cases}$$

From [12, Proposition 1.1] and [4], we have the following theorem.

Theorem 1.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\mathrm{tor}}$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for $5 \le n \le 10$, $n = 12$ or to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Then $|E(\mathbb{Q})_{\mathrm{tor}}| \mid m$ except for* "11*a*3", " 14*a*4", "14*a*6" *and* "20*a*2" *for which cases we have $|E(\mathbb{Q})_{\mathrm{tor}}| \mid c \cdot m$. Thus Conjecture* 2 *is true for these curves.*

So the only remaining cases for the validity of Conjecture 2 are those when $E(\mathbb{Q})_{\mathrm{tor}}$ is isomorphic to the following six groups: $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

In this paper, we prove the following theorem.

Theorem 1.2. *Let E be an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\mathrm{tor}}$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Then Conjecture* 2 *is true.*

Remark. Theorem 1.1 holds without any assumptions on K and P_K. When $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/3\mathbb{Z}$, most curves also satisfy $3 \mid m$ or $3 \mid c$ without any assumptions on K and P_K (cf. Proposition 3.1 or 3.2). But for the remaining elliptic curves E, we should show that $3 \mid m$ or $3 \mid |\text{Ш}(E/K)|^{1/2}$ under the assumption that $3 \nmid u_K$ and P_K has infinite order (cf. Proposition 3.3).

2. Preliminaries

For a positive integer N, let $X_1(N) = \mathbb{H}^*/\Gamma_1(N)$ and $X_0(N) = \mathbb{H}^*/\Gamma_0(N)$ denote the usual modular curves. Let $\mathcal{C}$ denote an isogeny class of elliptic curves defined over $\mathbb{Q}$ of conductor N. For $i = 0, 1$, there is a unique curve $E_i \in \mathcal{C}$ and a parametrization $\phi_i : X_i(N) \to E_i$ such that for any $E \in \mathcal{C}$ and parametrization $\phi'_i : X_i(N) \to E$, there is an isogeny $\pi_i : E_i \to E$ such that $\pi_i \circ \phi_i = \phi'_i$. For $i = 0, 1$, the curve E_i is called the $X_i(N)$-*optimal curve*.

In [2], Byeon and Yhee proved the following theorem which was conjectured by Stein and Watkins [16].

Theorem 2.1 ([2, Theorem 1.1(i)]). *For $i = 0, 1$, let E_i be the $X_i(N)$-optimal curve of an isogeny class $\mathcal{C}$ of elliptic curves defined over $\mathbb{Q}$ of conductor N. If there is an elliptic curve $E \in \mathcal{C}$ given by $E : y^2 + axy + y = x^3$ with discriminant $a^3 - 27 = (a-3)(a^2+3a+9)$, where a is an integer such that no prime factors of $a - 3$ are congruent to $1 \pmod 6$ and $a^2 + 3a + 9$ is a power of a prime number, then E_0 and E_1 differ by an isogeny of degree 3.*

For any $E \in \mathcal{C}$, we let $E_{\mathbb{Z}}$ be the Néron model over $\mathbb{Z}$ and ω_E a Néron differential on E. Let $\pi : E \to E'$ be an isogeny with $E, E' \in \mathcal{C}$. We say that π is *étale* if the extension $E_{\mathbb{Z}} \to E'_{\mathbb{Z}}$ to Néron models is étale. Equivalently, π is étale if $\ker \pi$ is an étale group scheme. So one can show that an isogeny $\pi : E \to E'$ is étale when $\ker \pi \cong \mathbb{Z}/p\mathbb{Z}$ as $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-modules and E has good reduction at p for an odd prime number p.

If $\pi : E \to E'$ is an isogeny over $\mathbb{Q}$, then we have $\pi^*(\omega_{E'}) = n\omega_E$ for some nonzero integer $n = n_\pi$. We note that the isogeny π is étale if and only if $n = \pm 1$. If $\pi : E \to E$ is the multiplication by an integer m, then $\pi^*(\omega_{E'}) = m\omega_E$. Thus if π is any isogeny of degree p for a prime number p and $\hat{\pi}$ denotes the dual isogeny, then $\hat{\pi} \circ \pi = [p]$, so $n_\pi = 1$ or p. It follows that precisely one of π and $\hat{\pi}$ is étale (cf. [18, Sec. 1]).

Stevens [17] proved that in every isogeny class $\mathcal{C}$ of elliptic curves defined over $\mathbb{Q}$, there exists a unique curve $E_{\min} \in \mathcal{C}$ such that for every $E \in \mathcal{C}$, there is an étale isogeny $\pi : E_{\min} \to E$. The curve $E_{\min}$ is called the *minimal curve* in $\mathcal{C}$. Stevens conjectured that $E_{\min} = E_1$ and Vatsal [18] proved the following theorem.

Theorem 2.2 ([18, Theorem 1.10]). *Suppose that the isogeny class $\mathcal{C}$ consists of semi-stable curves. The étale isogeny $\pi : E_{min} \to E_1$ has degree a power of 2.*

Let E be an elliptic curve defined over $\mathbb{Q}$ with a rational torsion point of order 3. As a minimal Weierstrass equation for E, we can take

$$E : y^2 + axy + by = x^3 \tag{1}$$

with $a, b \in \mathbb{Z}$, $b > 0$ such that for every prime number q, either $q \nmid a$ or $q^3 \nmid b$ (cf. [7, Sec. 1] or [11, Table 3]). The minimal discriminant Δ of E is

$$\Delta = b^3(a^3 - 27b)$$

and $T = \{(0,0),(0,-b),\infty\}$ is the torsion group of order 3. There is an isogeny defined over $\mathbb{Q}$ of degree 3 from E to the quotient curve E' of E by T and the curve E' is given by a Weierstrass eqation

$$E' : y^2 + axy + by = x^3 - 5abx - a^3b - 7b^2$$

with the discriminant Δ' is

$$\Delta' = b(a^3 - 27b)^3.$$

Hadano [7] obtained the following theorem.

Theorem 2.3 ([7, Theorem 1.1]). *The quotient curve E' of an elliptic curve $E : y^2 + axy + by = x^3$ by $T = \{(0,0),(0,-b),\infty\}$ has a rational point of order 3 if and only if b is a cubic number t^3, where t is a positive integer. Moreover, the curve E' is given by*

$$E' : y^2 + (a + 6t)xy + (a^2 + 3at + 9t^2)ty = x^3.$$

3. Proof of Theorem 1.2

First we prove the following proposition.

Proposition 3.1. *If an elliptic curve E is given by (1) such that a prime p divides b, then $3 \mid m_p$. Thus Conjecture 2 is true when $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/3\mathbb{Z}$.*

Proof. Let $P = (0,0)$ and $E_0(\mathbb{Q}_p)$ be the group of $\mathbb{Q}_p$-rational points of E which become non-singular points in the reduced curve $\tilde{E} : y^2 + \tilde{a}xy = x^3$ modulo p. Since P becomes singular, the class $P + E_0(\mathbb{Q}_p) \in E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ is non-trivial. Since $[3]P = O$, the identity element in $E(\mathbb{Q})$, the order of $P + E_0(\mathbb{Q}_p)$ is 3. Therefore, $3 \mid m_p = |E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)|$. □

From Proposition 3.1, we may assume $b = 1$, so E is given by the following minimal Weierstrass equation:

$$y^2 + axy + y = x^3 \tag{2}$$

with $a \in \mathbb{Z}$. Let $\mathcal{A}$ be the set of integers $a \in \mathbb{Z}$ satisfying

(i) $a \neq 3$ so that $\Delta \neq 0$,
(ii) no prime factors of $a - 3$ are congruent to $1 \pmod 6$,
(iii) $a^2 + 3a + 9$ is a power of a prime.

Proposition 3.2. *If an elliptic curve E is given by (2) with $a \in \mathcal{A}$, then $3 \mid c$. Thus Conjecture 2 is true when $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/3\mathbb{Z}$.*

Proof. First we assume that $a \neq -6, -3, -1, 0, 5$. Let $E \in \mathcal{C}$ be an elliptic curve given by (2) with the minimal discriminant $\Delta = a^3 - 27 = (a-3)(a^2+3a+9)$, where $a \in \mathcal{A}$.

By Theorem 2.3, the quotient curve E' of E by $T = \{(0,0), (0,-1), \infty\}$ has a rational point of order 3 and the equation of E' is given by

$$E' : y^2 + (a+6)xy + (a^2+3a+9)y = x^3.$$

The discriminant of Δ' of E' is $\Delta' = (a^3-27)^3$ and $T' = \{(0,0), (0, -(a^2+3a+9)), \infty\}$ is the torsion group of order 3 in $E'(\mathbb{Q})$. Since E' also has a rational point of order 3, we have the following étale 3-isogenies of elliptic curves:

$$E \to E' \to E''.$$

Since $(a+6)^3 - (a-3)^3 = 3^3(a^2+3a+9)$ and $a \neq -6, 3$, a^2+3a+9 cannot be a cube. So E'' has no rational points of order 3. Since $4x^3 + a^2x^2 + 2ax + 1 = 0$ has no rational solutions except for $a = -1, 5$, E has no rational points of order 2 by the duplication formula.

Let $C(E)$ denote the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in the isogeny class $\mathcal{C}$ of E. For a prime p, let $C_p(E)$ be the number of $\mathbb{Q}$-isomorphism classes of elliptic curves p-power isogenous to E. Then we have the product formula

$$C(E) = \prod_p C_p(E).$$

In [8], Kenku proved that $Y_0(N)(\mathbb{Q}) = \mathbb{H}/\Gamma_0(N)(\mathbb{Q})$ is empty except for $N \leq 19$, and $N = 21, 25, 27, 37, 43, 67$, and 163. This result implies that $C_3(E) \leq 4$. (For details, see [14, Proof of Theorem 5] and [8, Table in the proof of Theorem 2].) If there is an étale 3-isogeny $E''' \to E$ with $E''' : y^2 + Axy + B^3y = x^3$, then the discriminant $\Delta = a^3 - 3^3$ of E should be equal to $u^{-12}B^3(A^3 - 27B^3)^3$ for some $u \in \mathbb{Z}$, but it is impossible because $a \neq 0, 3$. Since E'' has no rational points of order 3, we have $C_3(E) = 3$. So Kenku's result above implies that $C_2(E) \leq 2$ and $C_p(E) = 1$ for any prime $p \neq 2, 3$ because 9, 18, and 27 are the only multiples of 9 on Kenku's list. Since E has no rational points of order 2, there is no 2-isogenous curve of E and we have $C_2(E) = 1$. By the above product formula, we have $C(E) = 3$. So the isogeny class $\mathcal{C}$ of E is

$$E \to E' \to E'',$$

where each arrow denotes an étale 3-isogeny. Thus E is $E_{\min}$ in $\mathcal{C}$.

Since $c_4 := a(a^3 - 24)$, E has multiplicative reduction at p for every prime factor $p \neq 3$ of Δ. If $3 \mid \Delta$, then $a \mid 3$ and $a^2 + 3a + 9$ should be a power of 3. But it is impossible because $a \neq -6, -3, 0, 3$. Thus $3 \nmid \Delta$ and E is semi-stable. By Theorem 2.2, $E = E_1$ and by Theorem 2.1, $E \neq E_0$. Since there is an étale isogeny $E_1 (= E) \to E_0$ of degree 3 and the Manin constant E is a nonzero integer c satisfying

$$\phi^*(\omega_E) = c\omega_f,$$

where $\phi : X_0(N) \to E$ is a modular parametrization and ω_f is the differential 1-form associated to a normalized newform f of level N (cf. [1]), we have $3 \mid c$.

Finally we note that the cases $a = -6, -3, -1, 0, 5$ give the curves "27a4" "54a3", "14a4", "27a3" and "14a6", respectively, for which curves we can check $3 \mid c$ by [4]. □

Proposition 3.3. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N given by* (2) *such that $a \in \mathbb{Z} \setminus \mathcal{A}$ and $a \neq 3$. Let K be an imaginary quadratic field, where all prime divisors of N split in K. Assume that K has discriminant other than -3,* i.e. *$u_K \neq 3$. If P_K has infinite order in $E(K)$ and $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/3\mathbb{Z}$, then 3 divides $m \cdot |\mathrm{III}((\mathrm{E/K})|^{1/2}$. Thus Conjecture 2 is true.*

Proof. Let π be an isogeny defined over $\mathbb{Q}$ of degree 3 from E to the quotient curve E' of E by $T = \{(0,0),(0,-1),\infty\}$ and $\hat{\pi} : E' \to E$ be the dual isogeny. Since $E[\pi] \cong \mathbb{Z}/3\mathbb{Z}$ as $\mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K})$-module, $E'[\hat{\pi}]$ is isomorphic to its dual μ_3 as $\mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K})$-module by Weil pairing (cf. [15, Remark 8.4]). Since K does not contain the third roots of unity, $E'(K)[\hat{\pi}]$ is trivial. Thus we have

$$\frac{|E(K)[\pi]|}{|E'(K)[\hat{\pi}]|} = 3. \tag{3}$$

By [5, Theorem 1.2] and the fact that π is étale, we have

$$\prod_{\nu} \frac{\displaystyle\int_{E'(K_\nu)} |\omega_{E'}|_\nu}{\displaystyle\int_{E(K_\nu)} |\omega_E|_\nu} = \frac{\displaystyle\int_{E'(\mathbb{C})} |\omega_{E'}|}{\displaystyle\int_{E(\mathbb{C})} |\omega_E|} = 3^{-1}\left|\frac{\pi^*(\omega_{E'})}{\omega_E}\right| = 3^{-1}, \tag{4}$$

where v runs through the infinite places of K.

Assume that $3 \nmid m$. For each place $\mathfrak{p}$ of K which divides N, let $m_{\mathfrak{p}} = |E(K_{\mathfrak{p}})/E_0(K_{\mathfrak{p}})|$, where $E_0(K_{\mathfrak{p}})$ is the set of points of $E(K_{\mathfrak{p}})$ with non-singular reduction. Since $\mathfrak{p} \cdot \bar{\mathfrak{p}} = p$, we see that $K_{\mathfrak{p}} = K_{\bar{\mathfrak{p}}} = \mathbb{Q}_p$ and $m_{\mathfrak{p}} = m_{\bar{\mathfrak{p}}} = m_p$. Thus our assumption is in fact

$$3 \nmid \prod_{\mathfrak{q}} m_{\mathfrak{q}}, \tag{5}$$

where $\mathfrak{q}$ runs through the finite places of K. Let $\mathrm{Sel}^{\pi}(\mathrm{E/K})$ be the π-Selmer group (for definition, see [9]) of E over K, $\mathrm{Sel}^{\hat{\pi}}(\mathrm{E'/K})$ the $\hat{\pi}$-Selmer group of E' over K and $m'_{\mathfrak{q}} = |E'(K_{\mathfrak{q}})/E'_0(K_{\mathfrak{q}})|$. Then from (3)–(5) and Cassels's theorem (cf. [3] or [9, Theorem 1]):

$$\frac{|\mathrm{Sel}^{\pi}(\mathrm{E/K})|}{|\mathrm{Sel}^{\hat{\pi}}(\mathrm{E'/K})|} = \frac{|E(K)[\pi]| \cdot \prod_{\nu} \int_{E'(K_\nu)} |\omega_{E'}|_\nu \cdot \prod_{\mathfrak{q}} m'_{\mathfrak{q}}}{|E'(K)[\hat{\pi}]| \cdot \prod_{\nu} \int_{E(K_\nu)} |\omega_E|_\nu \cdot \prod_{\mathfrak{q}} m_{\mathfrak{q}}},$$

we have

$$\dim_{\mathbb{F}_3} \mathrm{Sel}^{\pi}(\mathrm{E/K}) \geq \mathrm{ord}_3\left(\prod_{\mathfrak{q}} m'_{\mathfrak{q}}\right). \tag{6}$$

Suppose that there are at least two distinct primes p and q dividing a^2+3a+9. By Theorem 2.3 and Proposition 3.1, we have $3 \mid m'_p = m'_{\mathfrak{p}} = m'_{\bar{\mathfrak{p}}}$ and $3 \mid m'_q = m'_{\mathfrak{q}} = m'_{\bar{\mathfrak{q}}}$. Thus from (6), we have

$$\dim_{\mathbb{F}_3}\mathrm{Sel}^{\pi}(\mathrm{E}/\mathrm{K}) \geq 4.$$

Suppose that there is a prime p such that $p \mid (a-3)$ and $p \equiv 1 \pmod 6$. Then there is at least one prime $q \neq p$ such that $q \mid (a^2+3a+9)$. Again by Theorem 2.3 and Proposition 3.1, we have $3 \mid m'_q = m'_{\mathfrak{q}} = m'_{\bar{\mathfrak{q}}}$. Since the slopes of the tangent lines at the node $(-\frac{(a+6)^2}{9}, \frac{(a+6)^3}{27}) \in E'(\mathbb{F}_p)$ are $\frac{-3(a+6)\pm(a+6)\sqrt{-3}}{6} \in \mathbb{F}_p$, E' has split multiplicative reduction at p. Since $3 \mid \mathrm{ord_p}(\Delta') = -\mathrm{ord_p}(\mathrm{j}')$, where Δ' and j' are the discriminant and the j-invariant of E', respectively, we have $3 \mid m'_p = m'_{\mathfrak{p}} = m'_{\bar{\mathfrak{p}}}$ (cf. [15, Appendix C, Corollary 15.2.1]). Thus from (6), we have

$$\dim_{\mathbb{F}_3}\mathrm{Sel}^{\pi}(\mathrm{E}/\mathrm{K}) \geq 4.$$

From the following short exact sequence of G_K-modules

$$0 \to E[\pi] \to E[3] \xrightarrow{\pi} E'[\hat{\pi}] \to 0,$$

we have the following long exact sequence:

$$\cdots \to H^0(G_K, E'[\hat{\pi}]) \to H^1(G_K, E[\pi]) \xrightarrow{\imath} H^1(G_K, E[3]) \to \cdots.$$

Since $E'(K)[\hat{\pi}] = 0$, $\imath$ is injective and thus

$$\dim_{\mathbb{F}_3}\mathrm{Sel}^3(\mathrm{E}/\mathrm{K}) \geq \dim_{\mathbb{F}_3}\mathrm{Sel}^{\pi}(\mathrm{E}/\mathrm{K}).$$

Thus we conclude that for the two cases,

$$\dim_{\mathbb{F}_3}\mathrm{Sel}^3(\mathrm{E}/\mathrm{K}) \geq 4. \tag{7}$$

If $\dim_{\mathbb{F}_3}\mathrm{E}(\mathrm{K})[3] = 2$, then $\mu_3 \subset K$ (cf. [15, Corollary 8.1.1]), but it is contradiction. So we have $E(K)[3] \cong \mathbb{Z}/3\mathbb{Z}$. Since $E(K)$ has rank 1, we have

$$E(K)/3E(K) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

Thus the following descent exact sequence

$$0 \to E(K)/3E(K) \to \mathrm{Sel}^3(\mathrm{E}/\mathrm{K}) \to \mathrm{III}(\mathrm{E}/\mathrm{K})[3] \to 0$$

and (7) implies

$$\dim_{\mathbb{F}_3}\mathrm{III}(\mathrm{E}/\mathrm{K})[3] \geq 2$$

and therefore, $3 \mid |\mathrm{III}(\mathrm{E}/\mathrm{K})[3]|^{1/2}$. □

Proof of Theorem 1.2. Theorem 1.2 follows from Propositions 3.1–3.3. □

Acknowledgment

The authors thank the referees for their careful readings and many valuable suggestions.

References

[1] A. Agashe, K. Ribet and W. Stein, The Manin constant, *Pure Appl. Math. Quart.* **2** (2006) 617–636.

[2] D. Byeon and D. Yhee, Optimal curves differing by a 3-isogeny, *Acta Arith.* **158** (2013) 219–227.

[3] J. W. S. Cassels, Arithmetic on curves of genus 1, IV, Proof of the Hauptvermutung, *J. Reine Angew. Math.* **211** (1962) 95–112.

[4] J. Cremona, Elliptic curve data; http://johncremona.github.io/ecdata.

[5] T. Dokchitser and V. Dokchitser, Local invariants of isogenous elliptic curves, *Trans. Amer. Math. Soc.* **367** (2015) 4339–4358.

[6] B. H. Gross and D. Zagier, Heegner points and derivatives of L-series, *Invent. Math.* **84** (1986) 225–320.

[7] T. Hadano, Elliptic curves with torsion point, *Nagoya Math. J.* **66** (1977) 99–108.

[8] M. Kenku, On the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class, *J. Number Theory* **15** (1982) 199–202.

[9] R. Kloosterman and E. F. Schaefer, Selmer groups of elliptic curves that can be arbitrarily large, *J. Number Theory* **99** (2003) 148–163.

[10] V. Kolyvagin, Euler systems, in *The Grothendieck Festschrift*, Vol. II (Birkhäuser, Boston, MA, 1990), pp. 435–483.

[11] D. S. Kubert, Universal bounds on the torsion of elliptic curves, *Proc. Lond. Math. Soc.* **33** (1976) 193–237.

[12] D. Lorenzini, Torsion and Tamagawa numbers, *Ann. Inst. Fourier* **61** (2011) 1995–2037.

[13] B. Mazur, Modular curves and the Eisenstein ideal, *Publ. Math. Inst. Hautes. Études. Sci.* **47** (1977) 33–186.

[14] B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978) 129–162.

[15] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 2nd edition, Vol. 106 (Springer, New York, 2009).

[16] W. Stein and M. Watkins, A database of elliptic curves-first report, in *Algorithmic Number Theory* (*Sydney, 2002*), Lecture Notes in Computer Science, Vol. 2369 (Springer, Berlin, 2002), pp. 267–275.

[17] G. Stevens, Stickelberger elements and modular parametrizations of elliptic curves, *Invent. Math.* **98** (1989) 75–106.

[18] V. Vatsal, Multiplicative subgroup of $J_0(N)$ and applications to elliptic curves, *J. Inst. Math. Jussieu* **4** (2005) 281–316.